

PERSONAL COMPUTER (PC) INVENTORY  
FOLLOW-UP REPORT  
EXECUTIVE SUMMARY

## ***FTB's IT EQUIPMENT IS AT RISK!***

### **AUDIT HIGHLIGHTS**

Franchise Tax Board's (FTB) IT equipment have been tracked and maintained in the Unicenter database since the conversion from Track-It in August of 2007. There are approximately 14,600 desktops, laptops, miscellaneous equipment, servers, and monitors tracked in the Unicenter database. The IT Asset Management Unit, within the Enterprise Technology Management Bureau, tracks and inventories this information in the Unicenter database.

Our review, which includes a one-year follow-up review from a prior audit completed in May of 2007, revealed the following major areas of concern. For more detailed information, please refer to the audit report.

- FTB's IT assets are not adequately safeguarded against loss or theft
- The Unicenter database does not contain accurate information
- Procedures are not up-to-date

We recognize and commend the IT Asset Management Unit for their hard work in securing the equipment within the IT Warehouse. However, overall, the internal controls over the IT equipment remain weak and inadequate. These weak internal controls leave many opportunities for errors and irregularities to occur.

### **AUDITEE RESPONSE**

The Enterprise Technology Management Bureau, Privacy, Security, and Disclosure Bureau, and Computing Resources Bureau concurred with our recommendations and provided a response for their resolutions. Please refer to Auditee Response of this report.



chair **John Chiang**  
member **Judy Chu, PhD**  
member **Michael C. Genest**

State of California  
**Franchise Tax Board**

08.04.2008

To: Julie Moreno,  
DPM III, Acting Director, Enterprise Technology Management Bureau

Denise Mellor,  
Director, Privacy, Security, and Disclosure Bureau

Carol Meraji,  
Director, Computing Resources Bureau

From: Philip Yu

**Personal Computer (PC) Inventory Follow-up Report**  
**FTB's IT Equipment is at RISK!**

## Memorandum

### Introduction

We have completed our one-year follow-up review of the PC Inventory audit. The initial audit was completed in May of 2006. At that time we requested the auditees to provide a one-year update to the findings referenced in the final report. In May of 2007 the Enterprise Technology Management Bureau (ETMB) and the Privacy, Security, and Disclosure Bureau (PSDB) provided us an update of how the seven findings were addressed and the status of each of them.

The purpose of the current review, which occurred from November 2007 to March 2008, was to assess the business process changes made in response to the seven prior findings as well as to review laptop security and the requests for moves, installs, and repairing IT equipment through the IT Service Help Desk. The report will also provide detail on additional areas of concern in regards to the management of Franchise Tax Board's (FTB) Information Technology (IT) assets.

### Background

In August of 2007 the Track-It software application used to track IT assets was replaced with the Unicenter software application. The Track-It database contains all historical data and is still utilized by ETMB staff to obtain historical data if needed. Data was transferred from Track-It to Unicenter with the exception of the following:

- IT equipment with an inventory date older than December 31, 2005
- Non-trackable IT equipment such as keyboards and desktop printers
- Equipment which is no longer under warranty
- California Child Support Automation System (CCSAS) equipment. CCSAS now tracks their own equipment; however, the IT Warehouse stores both surplus and new equipment for CCSAS

Although the software tracking application has changed, the processes and areas regarding IT assets have generally remained the same. The areas responsible for the management of IT equipment are the Business and Human Resources Bureau, ETMB, Computing Resources Bureau, and the PSDB. Within each bureau are sections that perform tasks related to the management and physical inventory of IT equipment within the FTB:

#### Business and Human Resources Bureau

The Business Services Section (BSS), within the Business and Human Resources Bureau, provides office support services throughout the department. The Service & Supply Unit, under BSS, is the initial recipient of all IT equipment:

##### Service & Supply

Service & Supply receives all IT equipment in the California Warehouse, enters the applicable information into the Property Management database, and delivers it to the IT Warehouse for tagging and distribution. They also receive surveyed items from the ETMB and distribute them to local schools or recycling centers.

#### Enterprise Technology Management Bureau

The ETMB provides consolidated enterprise support and service functions for FTB's IT equipment. The sections within ETMB that perform the physical inventory and manage the IT equipment are the IT Asset Management (ITAM) Unit and the IT Service Desk Section (Service Desk).

##### IT Asset Management (ITAM)

ITAM provides "cradle to grave" management for all Enterprise IT hardware and software. Within the ITAM Unit is the IT Warehouse group, which houses all IT equipment and the Physical Inventory group, which conducts the physical inventory of all FTB IT equipment. Upon receipt of the IT equipment, IT Warehouse staff tags the equipment and inputs the critical data (product name, serial number, product key number, etc.) into the Unicenter database. Once the equipment is tracked in the Unicenter database, it is either distributed to FTB staff or stored in the IT Warehouse for future use.

##### IT Service Desk Section (Service Desk)

The Service Desk is the central point of contact for IT service support. Existing FTB equipment may need to be moved, fixed, or replaced throughout its existence. Any of these instances would be initiated by an FTB employee and executed by the Service Desk. Service Desk staff is responsible for IT service requests, such as password changes and reporting broken IT equipment. The section is also responsible for the evaluation, testing, acquisition, configuration, deployment, and movement of IT equipment and software. The Service Desk staff would perform the equipment moves and update the Unicenter database documenting the change/resolution.

### Computing Resources Bureau

The Computing Resources Bureau (CRB) has direct responsibility for providing essential technology support and services for all branches of the Franchise Tax Board, which include batch and online processes in a 24 x 7 x 365 environment. These central services include systems software support and development for our large scale mainframe computer operating systems, network communications software support, data management, storage and capacity planning, database management systems, and support functions.

#### Server Management

The Server Management Section provides Directory, Networking, Messaging, Data, Web Application, File, and Print Services to the Enterprise, plus external Web Application Services to California's taxpayers, via distributed Computing and Storage Devices. They provide these services using a combination of hardware and advanced network operating system software, and strive to provide the most stable, secure, and reliable services in an efficient manner.

### Privacy, Security, and Disclosure Bureau

The Worksite Security Section, within the PSDB, is responsible for the physical protection of State and Federal taxpayer information, FTB facilities, equipment, employees, etc.

#### Worksite Security

Worksite Security is the first area of contact when an FTB asset is lost, stolen, or destroyed. Worksite Security completes an incident report and forwards a copy of the report to ITAM and the Property Coordinator within the BSS. ITAM and BSS will update the Unicenter database and the Property Management Database with the survey information.

## **Scope**

The scope of this review included the activities from July 1, 2006 to March 14, 2008.

## **Objectives**

The objectives of this review were to assure:

- The findings and recommendations identified in our prior audit were adequately addressed
- The business process changes implemented by the ETMB and PSDB adequately secure FTB's IT assets
- Laptops (loaner laptops included) are secure
- The Change Order ticket process requesting moves, installs, and repairing IT equipment through the IT Service Help Desk has adequate controls

## Methodology

The auditors reviewed the prior year's findings and the business process changes implemented by the business areas. Discussions were held with the auditees to determine the progress made on the business process changes and performed additional testing to ensure the findings were adequately addressed.

A preliminary study was conducted to review and evaluate the internal control environment of laptops and Change Order tickets established by the IT Service Desk Section. Policies and procedures were requested from these areas and testing was performed.

## Results

In the one-year follow-up review provided by the ETMB and PSDB, they assured us that they fully addressed all seven findings; however, only three of the findings were adequately addressed. Five additional findings were identified in this current review. The four prior year's findings not adequately addressed and the five new findings identified in this current review are provided. For further information, please see the attached document.

F1	Finding	The prior year's finding, "The Track-It inventory database did not provide reliable property information" is still unresolved.
	Recommendation	ETMB: <ul style="list-style-type: none"><li>• Enterprise Technology Management Bureau (ETMB) staff should update the data in Unicenter immediately after equipment is moved or worked on.</li><li>• Unicenter Management should implement a change to the system prompting a "would you like to save" pop-up window in the application to ensure users save their changes in Unicenter.</li></ul>

F2	Finding	The prior year's finding, "Separation of duties does not exist for personnel within the warehouse in regards to the access to the Track-It inventory module and PC equipment. A plan, schedule, and procedures do not exist in regards to taking physical inventory" is still unresolved.
	Recommendation	<p>ETMB:</p> <ul style="list-style-type: none"> <li>The badge access report should be reviewed and updated quarterly by IT Warehouse management and Loaner Laptop room management. Individuals who do not need access to the IT Warehouse and the Loaner Laptop room should be removed.</li> <li>The IT Warehouse manager and the Loaner Laptop room manager should request the badge access reports, if not received from Worksite Security, on a quarterly basis.</li> <li>A physical inventory plan and time schedule should be documented and followed.</li> </ul> <p>PSDB:</p> <ul style="list-style-type: none"> <li>Worksite Security should provide the IT Warehouse manager and the Loaner Laptop room manager the badge access reports on a quarterly basis.</li> </ul> <p>ETMB &amp; CRB:</p> <ul style="list-style-type: none"> <li>FTB 7458, FTB Facility Access Request, should be completed and provided to Worksite Security whenever an individual transfers to another unit, separates from FTB, or job duties change that does not require access to the IT Warehouse or the Loaner Laptop room.</li> </ul>

F3	Finding	The prior year's finding, "Security did not always provide ITAM with the incident reports when PC equipment was involved; therefore, Track-It inventory was not always updated" is still unresolved.
	Recommendation	PSDB:  Worksite Security should provide ITAM and the BSS copies of the incident reports immediately after IT equipment is reported missing.

F4	Finding	<p>The prior year's finding, "There are several servers that cannot be located. In addition, some servers do not have system number, State of California tags, and visible serial numbers. Surveyed servers remain on the Track-IT inventory when they should not" is still unresolved.</p> <p>Servers are not inventoried and are not accurately accounted for in the Unicenter database. In addition, some employees have access to the server rooms that do not have a business need.</p>
	Recommendation	<p>ETMB:</p> <ul style="list-style-type: none"> <li>Physical inventory should be performed on all servers throughout FTB.</li> <li>Labels/scanable bar codes should be placed on all servers.</li> </ul> <p>CRB:</p> <ul style="list-style-type: none"> <li>The server areas should inform ITAM of any surplus servers they have in their possession.</li> <li>If the surplus server is no longer needed, it should be returned to the IT Warehouse.</li> <li>The managers of the server rooms should request the employee access reports, if not received from Worksite Security, on a quarterly basis. In addition, the reports should be reviewed and returned to Worksite Security to update server room access in regards to FTB and non-FTB individuals.</li> </ul> <p>PSDB:</p> <ul style="list-style-type: none"> <li>Worksite Security should provide the managers of the server rooms the employee access reports on a quarterly basis.</li> </ul>



F5	Finding	The technicians within the IT Service Desk Section are not updating Change Orders when completing the request.
	Recommendation	ETMB: <ul style="list-style-type: none"> <li>Supervisors should periodically review the open Change Orders for accuracy and clarity.</li> <li>IT Service Desk technicians should be trained on how to perform and complete a Change Order in Unicenter.</li> <li>Change Orders should be associated to a Configuration Item to provide prior history on the IT equipment.</li> <li>Quarterly reports should be obtained by the Enterprise Technology Management Bureau (ETMB) management for review of all opened Change Orders for closeout determination.</li> <li>ETMB staff should input clear notes in the Unicenter database.</li> </ul>
F6	Finding	Laptops are not properly safeguarded.
	Recommendation	ETMB: <ul style="list-style-type: none"> <li>Locking cables should be installed on all laptops within FTB for use.</li> <li>If cables are not available for all laptops, the guideline should be modified to state to secure all laptops in a locking cabinet when leaving the office overnight or for extended periods of time.</li> </ul>

F7	Finding	Some of the procedures within the Enterprise Technology Management Bureau (ETMB) related to inventorying IT equipment, managing IT equipment in the IT Warehouse and distribution of loaner laptops are outdated or are not documented.
	Recommendation	<p>ETMB:</p> <ul style="list-style-type: none"> <li>• All procedures should be written and updated to reflect current practices.</li> <li>• In addition, all procedures should be shared with, and available to, staff.</li> </ul>
F8	Finding	Some IT equipment are not locked in secure areas when not in use.
	Recommendation	<p>ETMB:</p> <ul style="list-style-type: none"> <li>• Once equipment is identified as needing to be returned to the IT Warehouse and is picked up by an IT Service Desk technician, Unicenter should be updated and the equipment taken directly to the IT Warehouse for storage.</li> <li>• All IT equipment transactions should be updated in Unicenter by the IT Service Desk technician immediately after equipment is picked up from/delivered to the IT Warehouse, training rooms, individual work stations, storage areas, etc.</li> <li>• The location code should be updated immediately after being moved/transferred.</li> <li>• Any lost or stolen equipment should be reported to Worksite Security immediately once it is identified as missing.</li> </ul>

F9	Finding	Separation of duties does not exist in regards to the IT Warehouse performing their own physical inventory on IT Warehouse equipment.
	Recommendation	ETMB:  An individual who does not work in the IT Warehouse should be performing the physical inventory.

### Conclusion

Improvements within the ITAM Unit have been made since the prior year's audit: The IT Warehouse staff has strengthened their internal controls, they are more organized, and more efficient with their processes. With the implementation of the Unicenter database it has been difficult for the ETMB to perform their duties as they did in the past; however, they are making great strides in learning the system.

Based on the results of our review, four of the seven prior findings were not adequately addressed and five additional findings were identified. The internal controls over the IT equipment remain weak and inadequate. These weak internal controls leave many opportunities for errors and irregularities to occur. Since we still found many pieces of equipment unaccounted for, it is critical that controls be implemented to safeguard the assets and maintain accurate records.

We have attached the responses from the ETMB, PSDB, and CRB which adequately address the deficiencies stated in our report. Please inform Internal Audit, in writing, of your efforts to implement the recommendations after 60-days, 6-months, and 1-year from the date of this final report. The information you provide us will be used to determine the need for a follow-up review.

We would like to thank you for the cooperation and assistance provided to us by your staff during our review. If you have any questions, please contact Sara Sheikholislam at 845-7973.

Philip Yu, Director  
Internal Audit Bureau

### Attachments

cc: S. Stanislaus  
L. Iwafuchi  
C. Cleek  
L. Crowe  
J. Sulenta  
R. Cartwright

## **FINDINGS & RECOMMENDATIONS**

**FINDING 1 (F-1):** The prior year's finding, "The Track-It inventory database did not provide reliable property information" is still unresolved.

**CONDITION:** The Track-It inventory database, containing all FTB IT equipment, was replaced in August of 2007 with a new database system referred to as Unicenter. A Unicenter database report dated November 2007 containing 14,014 desktops, laptops, miscellaneous equipment, and monitors was obtained, reviewed, and revealed the following:

One desktop had an inventory date of:	1/3/06
Inventory date prior to 1/1/07:	121
No evidence of inventory performed:	5
Missing location codes:	35
Missing serial numbers:	2
Location code of "In Transit to/from Warehouse":	477

A sample of 45 desktops, laptops, monitors, and miscellaneous equipment such as scanners and digital senders from the November 2007 Unicenter database report was selected to conduct a physical inventory to ensure the data within Unicenter matched the IT equipment on the floor. Nineteen pieces of equipment (42%) listed in Unicenter could not be physically located.

An additional Unicenter database report was generated on January 31, 2008 listing all equipment with a location code of "In Transit to/from Warehouse" because the volume of occurrences appeared to be significantly high from the November report. A total of 458 pieces of equipment with a location code of "In Transit to/from Warehouse" was on the January 31<sup>st</sup> report. Of these 458 items, 186 were correctly coded. Of the remaining 272 items, 10 were randomly selected. Of these 10, all had the incorrect location codes.

The auditors observed when sitting with the IT Warehouse staff that if the "save" button is not selected after making changes to the Unicenter system, the changes will not be saved. There is not an automatic save or a prompt to save changes.

**CRITERIA:** SAM Section 8650 states, "Departments will keep track of state property, whether capitalized or not, in an automated property accounting system (if one is used)."

**EFFECT:**

- It will be difficult or impossible to locate IT equipment with incorrect information in Unicenter. In addition, taking a physical inventory of IT equipment would be difficult to perform.

**(FINDING 1 (F-1) CONT)**

- The lack of control over the physical inventory could lead to future losses.
- Changes made to the system but not saved leaves the old data in the Unicenter database.

**CAUSE:** The Unicenter database is not being updated properly or at all.

**RECOMM-  
ENDATION:**

- Enterprise Technology Management Bureau (ETMB) staff should update the data in Unicenter immediately after equipment is moved or worked on.
- Unicenter Management should implement a change to the system prompting a “would you like to save” pop-up window in the application to ensure users save their changes in Unicenter.

**FINDING 2 (F-2):** The prior year's finding, "Separation of duties does not exist for personnel within the warehouse in regards to the access to the Track-It inventory module and PC equipment. A plan, schedule, and procedures do not exist in regards to taking physical inventory" is still unresolved.

**CONDITION:** The IT Warehouse is a limited access badge area. It is separated into three separate caged off areas belonging to IT Asset Management (ITAM), the Business Services Section (BSS), and Facilities. Each area has a lock combination entry gate for their caged area.

In the prior audit it was recommended that badge access and the lock combination code should only be given to the individuals working in Room 1300 (IT Warehouse) and Room 1300N, the Loaner Laptop room located at SF2D-A05-02, however this is not the case.

On a quarterly basis, Worksite Security is to provide the badge access area managers a list of individuals with access to the badged areas. It is the managing area's responsibility to provide guidance to Worksite Security as to who should be removed from the list.

#### Room 1300 (IT Warehouse)

Badge access is requested through an FTB Facility Access Request, FTB 7458. FTB 7458 is submitted to Worksite Security, within the Privacy, Security Disclosure Bureau (PSDB), who then activates badge access to specific areas for FTB staff.

An employee access report for Room 1300 (IT Warehouse) dated December 10, 2007, was obtained from Worksite Security. The report contains 43 individuals with access to Room 1300. Of the 43 individuals with access, four should be removed off the list.

#### Room 1300N (Loaner Laptop room)

Only employees who are in charge of the loaner laptop equipment and the Service and Warranty equipment should have access to the Loaner Laptop room.

An employee access report dated March 27, 2008 was obtained from Worksite Security for the Loaner Laptop room located at SF2D-A05-02, previously known as Room 1300N. The report lists 33 individuals with access to the Loaner Laptop room, 19 of which should be removed off the list.

#### Physical Inventory

It was also recommended in the prior audit that a plan and schedule for physical inventory be established and documented.

**(FINDING 2 (F-2) CONT)**

In this current review, a written plan and schedule were not provided to the auditor.

**CRITERIA:** SAM 8652 states, "Departments are responsible for developing and carrying out an inventory plan which include:

1. Inventory Taking:
  - a. Time schedule;
  - b. Count procedure (type of listing or count sheet to be used); and
  - c. Count assignment (statement of who will take the inventory at the times and locations scheduled).
2. Internal Control:
  - a. Inventories will not be exclusively controlled by the custodian of the property records;
  - b. Worksheets used to take inventory will be retained for audit and will show the date of inventory and the name of the inventory taker;
  - c. Inventory records will be retained in accordance with provisions of SAM Section 1671; and
  - d. The person in charge of the stockroom, if one is used, will not be in charge of maintaining the inventory records nor the taking of physical inventories;

**EFFECT:**

- Individuals who continue to have access to the IT Warehouse and Loaner Laptop room when there is no business need, increases the risk of IT equipment theft.
- Without an inventory plan or schedule there is a greater chance that the physical inventory of IT equipment will not be completed for the entire department and that it will not be done accurately; therefore, resulting in an inaccurate accounting of the department's IT equipment.

**CAUSE:**

- Worksite Security is not always providing the badge access reports to the Loaner Laptop room (SF2D-A05-02) manager on a consistent quarterly basis.
- Managers of the badge access areas are not providing Worksite Security with updates regarding who should be removed off the access list when the employee changes job duties, is deployed, or transferred.
- The inventory plan and schedule has not been documented.



(FINDING 2 (F-2) CONT)

**RECOMM-  
ENDATION:**

- Worksite Security should provide the IT Warehouse manager and the Loaner Laptop room manager the badge access reports on a quarterly basis.
- The IT Warehouse manager and the Loaner Laptop room manager should request the badge access reports, if not received from Worksite Security, on a quarterly basis.
- The badge access report should be reviewed and updated quarterly by IT Warehouse management and Loaner Laptop room management.
- Individuals who do not need access to the IT Warehouse and the Loaner Laptop room should be removed.
- FTB 7458, FTB Facility Access Request, should be completed and provided to Worksite Security whenever an individual transfers to another unit, separates from FTB, or job duties change that does not require access to the IT Warehouse or the Loaner Laptop room.
- A physical inventory plan and time schedule should be documented and followed.

**FINDING 3 (F-3):** The prior year's finding, "Security did not always provide ITAM with the incident reports when PC equipment was involved; therefore, Track-It inventory was not always updated" is still unresolved.

**CONDITION:** All lost or stolen IT equipment should be reported to Worksite Security within the Privacy, Security, and Disclosure Bureau. Worksite Security should prepare an incident report documenting the loss or theft. All incident reports involving the loss or theft of IT equipment should be forwarded to IT Asset Management (ITAM) and to the Business Services Section (BSS) in order for the equipment to be properly accounted for in the Unicenter database, which replaced Track-It in August 2007. Once ITAM and the BSS receive the incident report, ITAM should update the Unicenter database and the BSS should update the Property Management database.

From July 1, 2006 to November 6, 2007, Worksite Security had 14 reported incidents involving physical inventory. Equipment that is found, belongs to the Department of Child Support Services (DCSS), or non-inventoried equipment are not required to be reported to ITAM or the BSS. Incident reports involving inventoried IT equipment should be reported to ITAM and the BSS immediately, however this is not the case. Of the 14 reported incidents, ITAM received 3 but should have received a total of 12 incident reports regarding IT equipment. BSS received a total of 3 but should have received a total of 8 incident reports regarding IT equipment.

**CRITERIA:** The Theft, Loss, Damage or Destruction of State Property Guideline, located on the FTBNet Item #9, states that the Department Security Officer is to immediately inform and provide a copy of the incident report to ITAM and the BSS if the incident involves computer hardware or software.

**EFFECT:** When the incident reports are not provided to ITAM and the BSS, the Unicenter inventory database and the Property Management database are not updated to properly reflect IT inventory.

**CAUSE:** Due to an inadvertent oversight, Worksite Security did not provide the incident reports to ITAM and the BSS.

**RECOMM-  
ENDATION:** Worksite Security should provide ITAM and the BSS copies of the incident reports immediately after IT equipment is reported missing.

**FINDING 4 (F-4):** The prior year's finding, "There are several servers that cannot be located. In addition, some servers do not have system number, State of California tags, and visible serial numbers. Surveyed servers remain on the Track-IT inventory when they should not."

Servers are not inventoried and are not accurately accounted for in the Unicenter database. In addition, some employees have access to the server rooms that do not have a business need.

**CONDITION:** **Inventory of Servers**

A physical inventory of the servers is not performed. The only form of inventory performed is referred to as "pinging". Pinging identifies servers utilized on the FTB network through the use of computer software. Pinging does not provide the actual physical location of the server, it only indicates if the server is in use. When the server is identified through the pinging process, the IT Asset Management (ITAM) Unit manually updates the "Inventory Date" field in Unicenter, the new IT asset inventory database which replaced Track-It in August of 2007.

A Unicenter database report identified 575 servers as of November 2007. Of the 575 servers, 205 lack information required to maintain accurate records in Unicenter. Our review identified the following:

Number of servers	Issue
88	Missing location code of server in Unicenter
62	No inventory date of server noted in Unicenter
17	Missing serial numbers on servers
14	Missing bar codes on servers
13	Inventory date of server prior to 1/1/07 noted in Unicenter (One server had an inventory date of 4/30/02)
6	Server could not be physically located
4	Incorrect location code of server in Unicenter
1	Incorrect serial number on server
<b>205</b>	<b>Total</b>

**(FINDING 4 (F-4) CONT)**

It was also identified that the server areas keep unused (surplus) servers in their areas in the event that parts are needed for servers currently in use. However, ITAM is not notified of the location of the surplus servers and therefore, the Unicenter database is not properly updated to reflect the server's status and location.

**Server Room Access**

There is a lack of control over badge access to the server rooms. Badge access to the server rooms is requested through the FTB Facility Access Request (FTB 7458) form by a manager, which is then approved by the server room manager and submitted to Worksite Security, within the Privacy, Security, and Disclosure Bureau. Worksite Security activates the individual's badge granting access to the server room.

Worksite Security reports that they provide a list to server room managers containing the names of individuals with server room access on a quarterly basis for review. It appears as if multiple areas should be receiving the reports. Some areas are getting the reports on a consistent basis and some are not.

An employee access report, dated February 21, 2008, was obtained for the five server rooms throughout the department. The auditor selected the Los Angeles building server room located at Central Office to perform the testing. A total of 238 individuals have access to the server room. It was identified that 29 individuals should not have access to this server room because of job changes or transfers. Of the 238 individuals with server room access, 34 individuals are vendors, which are non-FTB employees.

**CRITERIA:**

SAM Section 8600 states, "Departments will make a physical count of all property and reconcile the count with accounting records at least once every three years. Inventory counting does not need to be performed at one time for an entire department's property. Departments may take a rotating inventory according to an inventory calendar."

The FTB Policy File, Information Security Policy, Section 230, Employee Separation and Transfers states, "When an employee leaves FTB, all access privileges must be immediately revoked or suspended. Internal employee transfers within FTB work units require reassessment of security and access privileges to ensure the privileges are appropriate for the new job assignment. Changes to the FTB employee's system and facility access (physical and logical) are the responsibility of the employee's supervisor or manager at the time of the separation or transfer. If the event is a transfer within FTB, the new supervisor or manager is responsible for establishing new security and access privileges consistent with the employee's job duties."

**(FINDING 4 (F-4) CON'T)**

**EFFECT:**

- By not performing a physical inventory, the department will be unaware of the number of servers we have and lack the ability to determine if any servers are missing.
- Inaccurate and unreliable information in Unicenter will result if ITAM is not notified of the status and location of surplus servers.
- Servers are not adequately safeguarded which could lead to potential tampering and/or theft when individuals that no longer require access to the server rooms continue to have access.

**CAUSE:**

- Performing a physical inventory on the servers has not been a priority for the ITAM Unit.
- Labels/scanable bar codes have not been placed on some of the servers.
- ITAM is not always notified when servers are transferred or are no longer in use.
- Worksite Security may not always provide the employee access reports to the managers of the server rooms.
- The managers of the server rooms may not be reviewing and updating the employee access reports.

**RECOMM-  
ENDATION:**

- Physical inventory should be performed on all servers throughout FTB.
- Labels/scanable bar codes should be placed on all servers.
- The server areas should inform ITAM of any surplus servers they have in their possession. If the surplus server is no longer needed, it should be returned to the IT Warehouse.
- Worksite Security should provide the managers of the server rooms the employee access reports on a quarterly basis.
- The managers of the server rooms should request the employee access reports, if not received from Worksite Security, on a quarterly basis. In addition, the reports should be reviewed and returned to Worksite Security to update server room access in regards to FTB and non-FTB individuals.

**FINDING 5 (F-5): The technicians within the IT Service Desk Section are not updating Change Orders when completing the request.**

**CONDITION:** When FTB staff contacts the Information Technology (IT) Service Desk Section for IT related issues such as moves, equipment replacement, or broken equipment, an IT Service Desk technician will identify the issue and create a Change Order within the Unicenter database (the IT asset database which replaced Track-It in August 2007).

In order for there to be a history trail, all Change Orders must be associated, or linked, to the equipment. Equipment in Unicenter is also referred to as a Configuration Item.

IT Warehouse staff was asked to retain a days worth of Change Orders. A sample of 10 Change Orders from February 21, 2008 was reviewed in order to identify if the Change Orders were properly documented and associated to the Configuration Item in Unicenter. The results of our review indicated:

- 3 out of 10 Change Orders were not associated to a Configuration Item
- All 10 Change Orders had the incorrect location of the Configuration Item

In addition, during the course of our review, it was observed that on numerous occasions IT Service Desk technicians did not associate the Configuration Item to the Change Order in Unicenter when swapping equipment or returning equipment to the IT Warehouse.

Additionally, there were instances where it took a long time to resolve a Change Order, Change Orders remained opened after the task was completed, or the Change Order was closed when the task was not completed. From a report of open Change Orders dated February 4, 2008, containing 577 open Change Orders, 9 Change Orders were initially sampled and the following was found:

- It took an average of 33 days to close the Change Order after the issue was resolved.
- Comments/notes placed on the Change Orders by the IT Service Desk technicians were unclear to the auditor and IT Warehouse staff.

**CRITERIA:** Service Desk Procedures for "Updating Physical Inventory Items" instructs staff to associate the Change Order to the Configuration Item in Unicenter.

**(FINDING 5 (F-5) CONT)**

**EFFECT:**

- When Change Orders are not updated on a timely basis it results in inaccurate information in the Unicenter inventory database.
- An audit history trail does not exist when Change Orders are not associated to a Configuration Item, therefore making it difficult to identify all the issues related to a particular piece of equipment.
- Unclear notes in the Unicenter database could require more time for the IT Service Desk technicians to understand the task. In addition, the technicians could ignore the Change Order because it is too difficult to understand or the wrong task could be completed.

**CAUSE:**

- Closing Change Orders is not a high priority for the IT Service Desk technicians
- Some technicians do not have access to the Unicenter database
- Staff are not adequately trained to use Unicenter

**RECOMM-  
ENDATION:**

- Supervisors should periodically review the open Change Orders for accuracy and clarity.
- IT Service Desk technicians should be trained on how to perform and complete a Change Order in Unicenter.
- Change Orders should be associated to a Configuration Item to provide prior history on the IT equipment.
- Quarterly reports should be obtained by the Enterprise Technology Management Bureau (ETMB) management for review of all opened Change Orders for closeout determination.
- ETMB staff should input clear notes in the Unicenter database.

**FINDING 6 (F-6): Laptops are not properly safeguarded.**

**CONDITION:** Prior to working hours a walk-through was performed at the Central Office on the first and second floors of the San Francisco building and a portion of the second floor of the Sacramento building to verify if guidelines were being followed to protect FTB laptops and the data they contain.

It was identified that seven laptops were not secured. The laptops were left out overnight on their unlocked docking stations.

**CRITERIA:** IT Service Desk Notebook/laptop security guidelines state, "When leaving it (notebook/laptop) at the office overnight or for other extended periods: Lock it in a cabinet and hide/take the key or secure it with a FTB issued locking cable and hide/take the key."

SAM section 5335.2 Personal Computer Security states, "Files containing confidential or sensitive data should not be stored in personal computer systems unless the agency can demonstrate that doing so is in the best interest of the state and that security measures have been implemented to provide adequate protection."

**EFFECT:** The laptops can be stolen or tampered with. In addition, confidential information can be disclosed, destructed, or altered.

**CAUSE:**

- Resources to purchase cables are not available at this time.
- Staff is negligent in locking up their equipment.

**RECOMM-  
ENDATION:**

Locking cables should be installed on all laptops within FTB for use. If cables are not available for all laptops, the guideline should be modified to state to secure all laptops in a locking cabinet when leaving the office overnight or for extended periods of time.



**FINDING 7 (F-7): Some of the procedures within the Enterprise Technology Management Bureau (ETMB) are outdated or are not documented.**

**CONDITION:** The Track-It inventory database, containing all FTB IT equipment, was replaced in August of 2007 with a new database system referred to as the Unicenter. All procedures throughout the ETMB required updating since the implementation of Unicenter, however this has not occurred. Procedures regarding physical inventory, the IT Warehouse, and Service and Warranty processes have not been updated.

Written procedures do not exist for distinguishing when loaner laptops are to be used, the duration of time they are loaned out for, what happens when one is lost, etc. In addition, written procedures do not exist for the loaner laptop check-in and check-out processes.

**CRITERIA:** As stated in SAM 20000, "Policies and procedures ensure management's directives are carried out and help ensure that necessary actions are taken to minimize risks to achievement of the entity's objectives".

SAM section 20050 states, "Each system an entity maintains to regulate and guide operations should be documented through flowcharts, narratives, desk procedures, and organizational charts."

**EFFECT:** There is the potential for loss of equipment and inaccurate inventorying of the loaner laptops.

There is the potential for inconsistent, incomplete, and/or incorrect completion of the processes.

**CAUSE:** Since the implementation of Unicenter, updating and/or documenting formal written procedures has not been a priority for staff.

**RECOMM-  
ENDATION:** All procedures should be written and updated to reflect current practices. In addition, all procedures should be shared with, and available to, staff.

**FINDING 8 (F-8): Some IT equipment are not locked in secure areas when not in use.**

**CONDITION:** After IT Service Desk Section technicians pick up equipment from an individual within FTB because it is no longer needed or it is not working properly, the technician places it on a table labeled "Return to IT Warehouse." This table is located in an unsecured aisle way on the second floor of the San Francisco building, Central Office, within the IT Service Desk area. All equipment placed on this table is taken to the IT Warehouse by IT Asset Management (ITAM) staff approximately three to four times a day.

An incident occurred where a piece of equipment was placed on the "Return to IT Warehouse" table but it never arrived at the IT Warehouse. This piece of equipment remains missing. The IT Service Desk did not report the missing equipment to Worksite Security until several weeks after identifying the equipment could not be found.

**CRITERIA:** As stated in the FTB Policy File, Information Security Policy, Section 440, "Physical security policies must be applied, at minimum, to all systems, storage media, and network components. All systems, storage media, and network components that are State-owned or owned by external entities providing FTB services, must be physically secured so that access is restricted to personnel authorized by the Data Owner."

**EFFECT:** Unsecured IT equipment could be stolen or misused and confidential/sensitive data could be manipulated, destructed, or disclosed.

**CAUSE:** IT Service Desk staff leave the IT equipment on the "Return IT Warehouse" table instead of taking the equipment to the IT Warehouse immediately.

**RECOMM-  
ENDATION:**

- Once equipment is identified as needing to be returned to the IT Warehouse and is picked up by an IT Service Desk technician, Unicenter should be updated and the equipment taken directly to the IT Warehouse for storage.
- All IT equipment transactions should be updated in Unicenter by the IT Service Desk technician immediately after equipment is picked up from/delivered to the IT Warehouse, training rooms, individual work stations, storage areas, etc. The location code should be updated with the newest location.
- Any lost or stolen equipment should be reported to Worksite Security immediately once it is identified as missing.

**FINDING 9 (F-9):** Separation of duties does not exist in regards to the IT Warehouse performing their own physical inventory on IT Warehouse equipment.

**CONDITION:** Physical Inventory of IT equipment in the IT Warehouse has been performed quarterly by the IT Warehouse Staff. Physical inventory has been performed on a non-work day in order to properly account for all inventory in the IT Warehouse. The equipment was scanned by a handheld scanner then loaded up to the Unicenter database (the new database system which replaced Track-It in August of 2007).

**CRITERIA:** SAM 8652 states, "The person in charge of the stockroom, if one is used, will not be in charge of maintaining the inventory records nor the taking of physical inventories."

**EFFECT:** The lack of separation of duties over the physical inventory could affect the reliability of the inventory database and could lead to future loss of equipment.

**CAUSE:** IT Warehouse staff was unaware that they should not be performing their own physical inventory.

**RECOMM-  
ENDATION:** IT Warehouse staff should not perform the physical inventory on the items in the IT Warehouse. An individual who does not work in the IT Warehouse should be performing the physical inventory.

## **RESPONSES TO RECOMMENDATIONS**



chair **John Chiang**  
member **Judy Chu, Ph.D.**  
member **Michael C. Genest**

State of California  
**Franchise Tax Board**

07.29.08

**Attachment B**

To: Philip Yu

Director, Internal Audit

From: Denise Mellor

Director, Privacy, Security & Disclosure Bureau

**Subject: PSDB Response To Findings And Recommendations Regarding The Personal Computer (PC) Inventory Follow Up Report**

## Memorandum

The following is in response to follow up report that was conducted in 2008 on the PC Inventory Audit.

Finding F-2 PSDB:

- Worksite Security should provide the appropriate designee the badge access report on a quarterly basis for the laptop loaner room located in the San Francisco building.

PSDB Response: Worksite Security has continued to provide quarterly reports for various areas to the IT Warehouse manager on a quarterly basis as required. However the report for the laptop loaner room has been provided on an inconsistent basis. Due to staffing changes, the point of contact for the laptop loaner room has changed without notice to Worksite Security. Worksite Security agrees to work with the IT Asset manager to identify a single point of contact to provide all reports to and then provide them on a consistent basis. Additionally, if the point of contact for the IT Asset Center changes, the IT Asset Center manager needs to provide Worksite Security with this information as soon as possible.

Finding F-3 PSDB:

- Worksite Security should provide ITAM and the BSS copies of the incident reports immediately after IT equipment is reported missing.

PSDB Response: The following actions have been taken to improve compliance in this area: 1. For closer supervision and increased accountability, Worksite Security now has a working level supervisor who has responsibility for this program. 2. Retraining on this procedure has been conducted. 3. To strengthen this procedure, a checklist has been created and added to the procedure for increased awareness and easier identification of where reports need to be sent.

Finding F-4 PSDB:

- Worksite Security should provide the manager of the server rooms the employee access reports on a quarterly basis.

PSDB Response: Worksite Security has continued to provide quarterly reports to various areas within the server rooms as required. However, the report to one of the program areas located inside the server room has been delivered inconsistent basis due to staffing changes. Issues exist due to multiple program areas located within the rooms secured by the badge readers in the server room areas. Per an agreement with Carol Meraji, Director for Computing Resources Bureau, the reports will be forwarded to a single point of contact, Dennis Mills. To streamline this process and strengthen access controls into this area, the newly identified point of contact will need to work closely with the other program areas to ensure only appropriate personnel have been assigned access into this secured area.

Denise Mellor  
Director, Privacy, Security & Disclosure Bureau

## Enterprise Technology Management Bureau Response to the Audit Findings

Internal Audit Findings	Owner	Deliverable	Due Date	Notes
F1 – UniCenter asset database does not provide reliable property information.	John Sulenta Julie Moreno	Procedures for UniCenter and asset tracking.	7-25-08 / Plan 9-1-08 / Procedures	Bill O'Brien will check on feasibility of "save" pop-up screen 7/28/08 – Bill O'Brien spoke with UniCenter admins via Change Order # 08-246163-2 (Closed 2/29/08) to discuss this request. We were told by CA that this could not be done at this time within the program. They advised that this may be fixed in future updates. UniCenter Admins will fix if update becomes available.
F2 – Separation of duties regarding access to UniCenter asset module and access to rooms with assets.	Larry Walker	Quarterly report of access rights to loaner laptop room. Ensure right employees have access.	7-25-08 / Plan 9-1-08 / Quarterly Report	7/28/08 – (Inventory Plan) - Bill O'Brien will be working with Hardware Management & Compliance Lead to discuss a documented plan on how we will perform physical inventories in the future. Plan will be provided NLT the 60 day follow-up to Internal Audit. (Badge Access Reports) – Bill

				O'Brien has been receiving periodic reports from security to verify access. In addition, Bill is working with Jim Shook to attempt to gain full rights to the IT Warehouse location.
F3 – Failure of security to provide ITAM with incident reports regarding assets.	N/A	N/A	N/A	7/28/08 – Bill O'Brien will work with Rebecca Cartwright and Cordis Clayton to improve this process.
F4 – Missing servers	N/A	N/A	N/A	7/28/08 – Matt Feaster has updated the majority of servers into UniCenter and is in the process of creating labels for all server equipment. Equipment should be labeled in the next 60 – 90 days once some data corrections can be completed in UniCenter.
F 5 – IT Service Desk not updating change orders when completing request.	Anthony Armstrong	Procedures	7-25-08 / Plan 9-01-08 / Procedures	Will work with KB SME's to publish in KB.  7/28/08 – This issue will be discussed with management to ensure that supervisors are performing quality review of their staff's work and that the proper



				procedures are in place and updated to ensure assets are being documented appropriately..
F6 – Laptop safeguards	Departmental issue	N/A	N/A	7/28/08 – We believe this is a departmental issue that needs to be addressed in a department wide policy from the CIO or the Executive Officer. We will forward this issue to Cathy Cleek and senior staff to discuss how to proceed. Update to be provided in the 60 day update to IA.
F7 – Procedures related to inventorying IT equipment and distribution of loaner laptops are outdated or do not exist.	Larry Walker	Procedures	7-25-08 / Plan 9-1-08 / Procedures	Larry to address only loaner laptops. Megan and Letty to publish in KB. 7/28/08 – IT Asset Management will continue to create and improve procedures to ensure that all workloads within Asset Management have a documented procedure to support how we conduct business.
F8 – IT equipment not locked in secure areas.	Mahmood Sitarian	Procedures and plan to address OAR storage	7-25-08 / Plan 9-01-08 / Procedures	Megan and Letty will publish in KB
F9 – Separation of duties does not	Bill O'Brien	N/A	N/A	7/28/08 – Bill O'Brien has

exist in physical inventory of warehouse				notified the Hardware Management & Compliance staff that they are now required to conduct the physical inventory of the IT Warehouse. This inventory will be included on the forthcoming Physical Inventory plan.
--	--	--	--	---



State of California  
**Franchise Tax Board**

07.21.08

**Attachment C**

To: Sara Sheikholislam  
From: Carol Meraji

**Response to PC Inventory Audit Report**

## **Memorandum**

### **Finding 4 (F4)**

**Issues:**

Unresolved from prior year's finding:

- Several servers cannot be located.
- Some servers do not have system number, State of California tags, and visible serial numbers.
- Surveyed servers remain on the Track-IT inventory when they should not.

This year:

- Servers are not inventoried and are not accurately accounted for in the Unicenter database.
- Some employees have access to the server rooms that do not have a business need.

**Recommendation:**

The server areas should inform ITAM of any surplus servers they have in their possession. If the surplus server is no longer needed, it should be returned to the IT Warehouse.

The managers of the server rooms should request the employee access reports, if not received from Worksite Security, on a quarterly basis. In addition, the reports should be reviewed and returned to Worksite Security to update server room access in regards to FTB and non-FTB individuals.

**Response:**

ISB agrees with the finding and recommendations.

- *ISB will education all managers, supervisors and leads to ensure that the survey process is understood and followed and servers that are no longer used are returned to the IT Warehouse.*
- *ISB Managers and Supervisors will work with Worksite Security on a quarterly basis to review that access to the Data Center raise floor areas is appropriate and revoke access if access is no longer required or if access was inappropriately provided.*
- *ISB will request support from asset and inventory staff in the new planning and operations bureaus to correctly tag and inventory all server equipment and have them update the Unicenter asset database as appropriate.*

## **Internal Audit (60 Day) Response (ITAM & ITSD)**

**F1** – The prior year’s finding, “The Track-It inventory database did not provide reliable property information” is still unresolved.

**ITAM Owner:** Julie Moreno

**ITAM Status:** **Closed**

**ITAM Resolution:**

**R1:** Procedures in ITAM require our staff to update assets as they are working on them. The process is being followed by ITAM staff.

**R2:** Bill O’Brien looked into the pop-up feature via the UniCenter Admins. The admins were unable to resolve. The admins contacted CA and were advised that this feature is not an option at this time. If it becomes an option, it will be implemented in a future UniCenter update.

**SD Owner:** John Sulenta

**SD Status:** **Closed**

**SD Resolution:**

**R1:** The team leads and supervisors continuously stress the importance of updating Unicenter when equipment is moved or worked on. Knowledgebase article 400051 identifies the steps to meet this objective.

**F2** – The prior year’s finding, “Separation of duties does not exist for personnel within the warehouse in regards to the access to the Track-It inventory module and PC equipment. A plan, schedule, and procedures do not exist in regards to taking physical inventory” is still unresolved.

**ITAM Owner:** Bill O’Brien

**ITAM Status:** **Closed**

**ITAM Resolution:**

**R1:** The IT Warehouse manager will be reviewing access to the IT Warehouse on a quarterly basis with security. Greg Wesley-Smith will be sending these reports to Bill O’Brien for verification.

**R2:** If the access reports are not received, the IT Warehouse manager will be proactive and request the report from security.

**R3:** The HW Mgmt & Compliance lead has updated our physical inventory procedures. In addition, she has created a plan that schedules when we should be conducting physical inventory in specific areas.

Currently, Central Office staff complete a continuous inventory of IT equipment based on the following calendar:

Jan – March: San Diego Bldg, Room 1300, California Warehouse, Security

April – June: Sacramento Bldg

July – September: Los Angeles Bldg

October – December: San Francisco Bldg, Town Center

**R4:** N/A

**R5:** FTB 7458 will be used for any changes to room access as required.

**SD Owner:** Larry Walker

**SD Status:** **Closed**

**SD Resolution:**

**R2:** The Workstation Support Team is currently requesting quarterly reports from security to review badge access.

**F3** – The prior year’s finding, “Security did not always provide ITAM with the incident reports when PC equipment was involved; therefore, Track-It inventory was not always updated” is still unresolved.

**PSDB Owner:** Rebecca Cartwright (PSDB)

**F4** – The prior year’s finding, “There are several servers that cannot be located. In addition, some servers do not have system number, State of California tags, and visible serial numbers. Surveyed servers remain on the Track-It inventory when they should not” is still unresolved

**ITAM Owner:** Bill O’Brien

**ITAM Status:** In-Process

**ITAM Resolution:**

**R1:** Server inventory has been taking place over the past year. There were numerous issues that needed to be resolved. Currently, we are approximately 60% complete. Due to in-depth research requirements and limited staff availability, we are projecting this inventory will take another 60 – 90 days before completion.

**R2:** All new server/network equipment is required to go through the product check-in group within the IT Asset Management Unit. Once new equipment is received we label according to SAM, enter the equipment into UniCenter and then release to the owning PUC.

For older equipment (already in production) we are going back and re-labeling any asset that does not have a label. This process will be completed with R1 (above).

**R3:** CRB

**R4:** CRB

**R5:** CRB

**R6:** PSDB

**CRB Owner:** Carol Meraji

**PSDB Owner:** Rebecca Cartwright

**F5** – The technicians within the IT Service Desk Section are not updating Change Orders when completing the request.

**SD Owner:** Anthony Armstrong

**SD Status:** In-process

**SD Resolution:**

**R1:** Change order queues are reviewed on a regular basis by the leads in Workstation Support and the OAR Deployment team. However, a formal quarterly review process is in development.

**R2:** Change order training is given to staff. Knowledgebase article 400051 describes this process in detail.

**R3:** This is now being done by staff and documented in Knowledgebase article 400051.

**R4:** This is being done a daily basis. Unicenter Dashboard can run a query for managers upon request. A formal quarterly report is in development.

**R5:** This is stressed by both management and leads.

**F6** – Laptops are not properly safeguarded.

**ITAM Owner:** Bill O’Brien

**ITAM Status:** In-Process

**ITAM Resolution:**

**R1:** Locking cables are now provided with all laptops. ITAM feels it is each individual’s responsibility to use their cable locks at work and off campus. If there are any individuals that do not have a cable lock, their PC Coordinator can submit a request through the SD and we will provide one for them.

**R2:** Regardless if a cable lock is provided or not, all laptops should be locked in a cabinet over night. This will be instructed in our next training session with the PC Coordinators. In addition, our Communicate IT team will work with Security and the IT SD to change the verbiage on their websites to include this direction.

**F7** – Some of the procedures within the Enterprise Technology Management Bureau (ETMB) related to inventorying IT equipment, managing IT equipment in the IT Warehouse and distribution of loaner laptops are outdated or not documented.

**ITAM Owner:** Bill O'Brien

**ITAM Status:** In-Process

**ITAM Resolution:**

**R1:** The IT Warehouse has most procedures written and posted on the "Y" drive. The IT Warehouse lead is still working on procedures for: Shipping Process & IT Warehouse Survey Process.

**R2:** These procedures are being collected on the "Y" drive and will be posted in our Knowledge Base within UniCenter.

**SD Owner:** Larry Walker

**SD Status:** Closed

**SD Resolution:**

**R1:** Procedures for requesting loaner laptops are completed and available for staff.

**R2:** Procedures for requesting loaner laptops are completed and available for staff.

**F8** – Some IT equipment are not locked in secure areas when not in use.

**SD Owner:** Mahmood Sitarian

**SD Status:** In-process

**SD Resolution:**

**R1:** This is being done and documented by a process flowchart. This flowchart is completed and will be published in the Knowledgebase.

**R2:** This is currently not being done by deployment staff as current staffing levels do not allow for this additional step to be performed. As asset management tools are improved and processes refined, efficiencies realized can be used in this effort. Additionally, "right in time" deployment greatly reduces the gap in time between the assets leaving the warehouse to the deployment to the end user. A crystal report may be created to identify assets in transit to help reconcile inventory.

**R3:** This is being done by the OAR Deployment staff upon delivery of the asset to the customer.

**R4:** This is currently being done by all staff and documented in Knowledgebase article 40280.

**F9** – Separation of duties does not exist in regards to the IT warehouse performing their own physical inventory on IT Warehouse equipment.

**ITAM Owner:** Bill O'Brien

**ITAM Status:** Closed

**ITAM Resolution:**

**R1:** This practice has been changed and the physical inventory of the IT Warehouse equipment will now be conducted by the HW Management and Compliance staff.



chair **John Chiang**  
member **Judy Chu, Ph.D.**  
member **Michael C. Genest**

State of California  
**Franchise Tax Board**

12.03.2008

To: Philip Yu Director, Internal Audit

From: Denise Mellor Director, Privacy Security & Disclosure Bureau

**Subject: PSDB 60-Day Response to PC Inventory Follow Up Report**

## Memorandum

The following is in response to the request for 60-day follow up information regarding the above referenced audit. The responses below include the original findings and PSDB responses:

Finding F-2 PSDB:

- Worksite Security should provide the appropriate designee the badge access report on a quarterly basis for the laptop loaner room located in the San Francisco building.

PSDB Response: Worksite Security has continued to provide quarterly reports for various areas to the IT Warehouse manager on a quarterly basis as required. However the report for the laptop loaner room has been provided on an inconsistent basis. Due to staffing changes, the point of contact for the laptop loaner room has changed without notice to Worksite Security. Worksite Security agrees to work with the IT Asset manager to identify a single point of contact to provide all reports to and then provide them on a consistent basis. Additionally, if the point of contact for the IT Asset Center changes, the IT Asset Center manager needs to provide Worksite Security with this information as soon as possible.

**60-Day Update:**

The IT Asset Center has provided a point of contact for Worksite Security to send these reports to. The process is now working as intended.

**Finding F-3 PSDB:**

- Worksite Security should provide ITAM and the BSS copies of the incident reports immediately after IT equipment is reported missing.

PSDB Response: The following actions have been taken to improve compliance in this area: 1. For closer supervision and increased accountability, Worksite Security now has a working level supervisor who has responsibility for this program. 2. Retraining on this procedure has been conducted. 3. To strengthen this procedure, a checklist has been created and added to the procedure for increased awareness and easier identification of where reports need to be sent.

**60-Day Update:**

The new, improved process with the checklist has been implemented and is currently being utilized.

**Finding F-4 PSDB:**

- Worksite Security should provide the manager of the server rooms the employee access reports on a quarterly basis.

PSDB Response: Worksite Security has continued to provide quarterly reports to various areas within the server rooms as required. However, the report to one of the program areas located inside the server room has been delivered inconsistent basis due to staffing changes. Issues exist due to multiple program areas located within the rooms secured by the badge readers in the server room areas. Per an agreement with Carol Meraji, Director for Computing Resources Bureau, the reports will be forwarded to a single point of contact, Dennis Mills. To streamline this process and strengthen access controls into this area, the newly identified point of contact will need to work closely with the other program areas to ensure only appropriate personnel have been assigned access into this secured area.

**60-Day Update:**

The above-mentioned agreement has been put into place. The process is now working as intended with the new point of contact receiving and returning the reports to Worksite Security.

Denise Mellor

Director, Privacy, Security & Disclosure Bureau





chair **John Chiang**  
member **Betty T. Yee**  
member **Michael C. Genest**

State of California  
**Franchise Tax Board**

02.26.2009

To: Philip Yu Director, Internal Audit

From: Denise Mellor Director, Privacy Security & Disclosure Bureau

**Subject: PSDB Six-Month Response to PC Inventory Follow Up Report**

## Memorandum

The following is in response to the request for 6-month follow up information regarding the above referenced audit. The responses below include the original findings and PSDB responses:

**Finding F-2 PSDB:**

- Worksite Security should provide the appropriate designee the badge access report on a quarterly basis for the laptop loaner room located in the San Francisco building.

PSDB Response: Worksite Security has continued to provide quarterly reports for various areas to the IT Warehouse manager on a quarterly basis as required. However the report for the laptop loaner room has been provided on an inconsistent basis. Due to staffing changes, the point of contact for the laptop loaner room has changed without notice to Worksite Security. Worksite Security agrees to work with the IT Asset manager to identify a single point of contact to provide all reports to and then provide them on a consistent basis. Additionally, if the point of contact for the IT Asset Center changes, the IT Asset Center manager needs to provide Worksite Security with this information as soon as possible.

**60-Day Update:**

The IT Asset Center has provided a point of contact for Worksite Security to send these reports to. The process is now working as intended.

**6-Month Update:**

The process continues to work as intended.

Finding F-3 PSDB:

- Worksite Security should provide ITAM and the BSS copies of the incident reports immediately after IT equipment is reported missing.

PSDB Response: The following actions have been taken to improve compliance in this area: 1. For closer supervision and increased accountability, Worksite Security now has a working level supervisor who has responsibility for this program. 2. Retraining on this procedure has been conducted. 3. To strengthen this procedure, a checklist has been created and added to the procedure for increased awareness and easier identification of where reports need to be sent.

**60-Day Update:**

The new, improved process with the checklist has been implemented and is currently being utilized.

**6-Month Update:**

The process is working as intended.

Finding F-4 PSDB:

- Worksite Security should provide the manager of the server rooms the employee access reports on a quarterly basis.

PSDB Response: Worksite Security has continued to provide quarterly reports to various areas within the server rooms as required. However, the report to one of the program areas located inside the server room has been delivered inconsistent basis due to staffing changes. Issues exist due to multiple program areas located within the rooms secured by the badge readers in the server room areas. Per an agreement with Carol Meraji, Director for Computing Resources Bureau, the reports will be forwarded to a single point of contact, Dennis Mills. To streamline this process and strengthen access controls into this area, the newly identified point of contact will need to work closely with the other program areas to ensure only appropriate personnel have been assigned access into this secured area.

**60-Day Update:**

The above-mentioned agreement has been put into place. The process is now working as intended with the new point of contact receiving and returning the reports to Worksite Security.

**6-Month Update:**

The process is working as intended.

Denise Mellor

Director, Privacy, Security & Disclosure Bureau

## **Internal Audit (1 Year) Final Response (ITAM & ITSD)**

**F1** – The prior year’s finding, “The Track-It inventory database did not provide reliable property information” is still unresolved.

**R1:** Enterprise Technology Management Bureau (ETMB) staff should update the data in UniCenter immediately after equipment is moved or worked on.

**R2:** UniCenter Management should implement a change to the system prompting a “would you like to save” pop-up window in the application to ensure users save their changes in UniCenter.

**ITAM Owner:** Julie Moreno

**ITAM Status:** **CLOSED**

**ITAM Resolution:**

**60 Day Response:**

**R1:** Procedures in IT Asset Management (ITAM) require our staff to update assets as they are working on them. These procedures are being followed by ITAM staff. **CLOSED**

**R2:** Bill O’Brien looked into the pop-up feature via the UniCenter Admins. The admins were unable to resolve. The admins contacted CA and were advised that this feature is not an option at this time. If it becomes an option, it will be implemented in a future UniCenter update. **CLOSED**

**SD Owner:** John Sulenta

**SD Status:** **CLOSED**

**SD Resolution:**

**60 Day Response:**

**R1:** The team leads and supervisors continuously stress the importance of updating Unicenter when equipment is moved or worked on. Knowledgebase article 400051 identifies the steps to meet this objective. **CLOSED**

**F2** – The prior year’s finding, “Separation of duties does not exist for personnel within the warehouse in regards to the access to the Track-It inventory module and PC equipment. A plan, schedule, and procedures do not exist in regards to taking physical inventory” is still unresolved.

**R1:** The badge access report should be reviewed and updated quarterly by the IT Warehouse management and Loaner Laptop room management. Individuals who do not need access to the IT Warehouse and the Loaner Laptop room should be removed.

**R2:** The IT Warehouse manager and the Loaner Laptop room manager should request the badge access reports, if not received from Worksite Security, on a quarterly basis.

**R3:** A physical inventory plan and time schedule should be documented and followed.

**R4:** **PSDB**

**R5:** FTB 7458, FTB Facility Access Request, should be completed and provided to Worksite Security whenever an individual transfers to another unit, separates from FTB, or job duties change that does not require access to the IT Warehouse or the Loaner Laptop room.

**ITAM Owner:** Bill O’Brien

**ITAM Status:** **CLOSED**

**ITAM Resolution:**

**60 Day Response:**

**R1:** The IT Warehouse manager will be reviewing access to the IT Warehouse on a quarterly basis with security. Greg Wesley-Smith will be sending these reports to Bill O’Brien for verification. **CLOSED**

**R2:** If the access reports are not received, the IT Warehouse manager will be proactive and request the report from security. **CLOSED**

**R3:** The HW Mgmt & Compliance lead has updated our physical inventory procedures. In addition, she has created a plan that schedules when we should be conducting physical inventory in specific areas. Currently, Central Office staff complete a continuous inventory of IT equipment based on the following calendar:

Jan – March: San Diego Bldg, Room 1300, California Warehouse, Security

April – June: Sacramento Bldg

July – September: Los Angeles Bldg

October – December: San Francisco Bldg, Town Center

**CLOSED**

**R4:** N/A

**R5:** FTB 7458 will be used for any changes to room access as required. **CLOSED**

**SD Owner:** Larry Walker

**SD Status:** **CLOSED**

**SD Resolution:**

**60 Day Response:**

**R2:** The Workstation Support Team is currently requesting quarterly reports from security to review badge access. **CLOSED**

**R5:** FTB 7458 will be used for any changes to room access as required. **CLOSED**

**F3** – The prior year’s finding, “Security did not always provide ITAM with the incident reports when PC equipment was involved; therefore, Track-It inventory was not always updated” is still unresolved.

**PSDB Owner:** Rebecca Cartwright (PSDB)

**R1: PSDB owns this finding.**

**F4** – The prior year’s finding, “There are several servers that cannot be located. In addition, some servers do not have system number, State of California tags, and visible serial numbers. Surveyed servers remain on the Track-It inventory when they should not” is still unresolved.

**R1:** Physical inventory should be performed on all servers throughout FTB.

**R2:** Labels/scannable bar codes should be placed on all servers.

**R3:** CRB

**R4:** CRB

**R5:** CRB

**R6:** PSDB

**ITAM Owner:** Bill O’Brien

**ITAM Status:** **In-Process, remaining portions will be handled in the asset reengineering process improvement that ISB and OMB are working on together. The effort is scheduled to start in early 2010.**

**ITAM Resolution:**

**60 Day Response:**

**R1:** Server inventory has been taking place over the past year. There were numerous issues that needed to be resolved. Currently, we are approximately 60% complete. Due to in-depth research requirements and limited staff availability, we are projecting this inventory will take another 60 – 90 days before completion.

**R2:** All new server/network equipment is required to go through the product check-in group within the IT Asset Management Unit. Once new equipment is received we label according to SAM, enter the equipment into UniCenter and then release to the owning PUC.

For older equipment (already in production) we are going back and re-labeling any asset that does not have a label. This process will be completed with R1 (above).

**6 Month Update (R1/R2):**

**R1/R2:**

Server Inventory Update - 05/14/09:

- 635 total server assets (Windows and UNIX) in Unicenter.
- 97% of server assets have a current inventory date and location (Current date = December 2008 to present.)

- 100% of (located) server assets, both at central office and in the field, have been labeled/re-labeled and inventoried from December 2008 to present.

As of 05/14/09 there are 19 servers in UAPM that do not have a current inventory date. Of these 19, 13 have no inventory date at all. (Meaning, they have not been seen since prior to the Track-It – Unicenter conversion.) An additional 2 of these 19 assets have inventory dates in June 2007, but are listed as “place holders” so we cannot say if we actually had these items or not. They could possibly have been created in Track-It in error and converted to Unicenter. Hardware management has not been able to locate these 2 items despite multiple full physical inventories of all server equipment. There are 4 items with inventory dates in 2008 that were not located during the last full physical inventory done from Dec. 2008 to present. These items may well be here, but were moving during the inventory time and have not yet been located. This is a good example of the point that physical inventory of IT assets is somewhat of a “moving target” with respect to having a 100% accurate inventory. We may very well come across these items in the future as we do inventory again. Hardware management is currently gathering testimonials from business areas about the servers that we consider “missing”. We have searched our entire Central Office Campus (including locked storage rooms, under desks, etc.) and have had no success in locating these items. Once we have received testimonials from the business areas about this equipment, we will begin working with security to survey these items as “lost/stolen”.

#### 1 Year Update:

**R1:** A full physical inventory has been performed on all server equipment throughout FTB. At present, there are 645 server assets in Unicenter. Of those, 97% have a current inventory date and location. (Current date is 12/08 to present.)

**R2:** All servers are now labeled with scannable bar code labels.

**R3: CRB**

**R4: CRB**

**R5: CRB**

**R6: PSDB**

**CRB Owner:** Carol Meraji

**PSDB Owner:** Rebecca Cartwright

**F5** – The technicians within the IT Service Desk Section are not updating Change Orders when completing the request.

**R1:** Supervisors should periodically review the open Change Orders for accuracy and clarity.

**R2:** IT Service Desk technicians should be trained on how to perform and complete a Change Order in UniCenter.

**R3:** Change Orders should be associated to a Configuration Item to provide prior history on the IT equipment.

**R4:** Quarterly reports should be obtained by the Enterprise Technology Management Bureau (ETMB) management for review of all opened Change Orders for closeout determination.

**R5:** ETMB staff should input clear notes in the UniCenter database.

**SD Owner:** Anthony Armstrong

**SD Status:** **CLOSED**

**SD Resolution:**

#### 60 Day Response:

**R1:** Change order queues are reviewed on a regular basis by the leads in Workstation Support and the OAR Deployment team. However, a formal quarterly review process is in development. **CLOSED**

**R2:** Change order training is given to staff. Knowledgebase article 400051 describes this process in detail. **CLOSED**

**R3:** This is now being done by staff and documented in Knowledgebase article 400051. **CLOSED**

**R4:** This is being done a daily basis. Unicenter Dashboard can run a query for managers upon request. A formal quarterly report is in development. **CLOSED**

**R5:** This is stressed by both management and leads. **CLOSED**

**6 Month Response:**

**R1-R5:** A formal quarterly review process has been developed and is in production. To ensure Change Order entitlement issues are expedited immediately, emails are being sent directly to the leads and managers notifying them of CO number and what needs to be resolved. The managers will continue to send monthly messages reminding staff on the importance of software entitlement and compliance. In addition, a bi-annual software entitlement report will also be requested to establish our continued progress.

**1 Year Update:**

**R1- R5:** At the beginning of each month, a list of all open Change Orders are sent to the manager and lead of appropriate Service Desk units. The list is reviewed and the appropriate Change Orders are closed or updated. **CLOSED**

**F6** – Laptops are not properly safeguarded.

**R1:** Locking cables should be installed on all laptops within FTB for use.

**R2:** If cables are not available for all laptops, the guideline should be modified to state to secure all laptops in a locking cabinet when leaving the office overnight or for extended periods of time.

**ITAM Owner:** Bill O'Brien

**ITAM Status:** **CLOSED**

**ITAM Resolution:**

**60 Day Response:**

**R1:** Locking cables are now provided with all laptops. ITAM feels it is each individual's responsibility to use their cable locks at work and off campus. If there are any individuals that do not have a cable lock, their PC Coordinator can submit a request through the SD and we will provide one for them.

**R2:** Regardless if a cable lock is provided or not, all laptops should be locked in a cabinet over night. This will be instructed in our next training session with the PC Coordinators. In addition, our Communicate IT team will work with Security and the IT SD to change the verbiage on their websites to include this direction.

**6 Month Response:**

**R1:** Closed

**R2:** Julie Moreno has recently sent out a message to the Operation's Management Bureau (OMB) staff (formerly ETMB). A similar message adjusted to address all users will be sent out to the department through a Communicate IT message within the next 60 days. Here is what the message said:

As the custodians of FTB's IT hardware assets, we all have a keen interest in ensuring hardware is managed properly. Due to recent thefts and vandalism, soon we will be asking all FTB to better secure notebook computers. Starting today, if you are a notebook user, please:

**When you leave for the day:**

- ❑ **And you are not taking your notebook with you,** lock your notebook away in one of your locking storage units. Remember to secure the keys (e.g., by taking them with you). You may also want to arrange for your supervisor to secure your second key as a backup. If you do not have keys to your storage units, contact your supervisor who will in turn arrange with Facilities to provide you keys.

- ❓ **If you are taking your notebook with you**, reconsider if you really need to take it away from the office. If you do, always store it in a secure, out-of-sight location when traveling (e.g., in the trunk of the car) and at your destination.

We know that many of you are already exemplary in securing your notebook. So this is just a reminder about the seriousness, as losses are reported to and investigated internally and potentially by the CHP. As well, failure to act responsibly in this matter may result in disciplinary action.

**See all the Notebook Guidelines:**

\*\*\*\*\*

**Do you still need a notebook computer?** If you no longer need a notebook computer, please contact your PC coordinator to arrange a trade-in for a desktop system. We're still offering faster desktops for much needed notebooks.

**Feedback?** Since we're the first to implement this requirement, we'd like your feedback so we can learn about any issues prior to implementing enterprise wide. That way we can make adjustments to the process, making it as easy to implement as possible. If you have feedback, please let your supervisor know.

Thank you for being exemplary in this matter.

Regards,

OMB Management Team

**1 Year Update:**

**R2: The following Communicate IT article has been written and sent to All FTB staff:**

\*\*\*\*\*

CLOSED

**F7** – Some of the procedures within the Enterprise Technology Management Bureau (ETMB) related to inventorying IT equipment, managing IT equipment in the IT Warehouse and distribution of loaner laptops are outdated or not documented.

**R1:** All procedures should be written and updated to reflect current practices.

**R2:** In addition, all procedures should be shared with, and available to, staff.

**ITAM Owner:** Bill O'Brien

**ITAM Status:** **CLOSED**

**ITAM Resolution:**

**60 Day Response:**

**R1:** The IT Warehouse has most procedures written and posted on the "Y" drive. The IT Warehouse lead is still working on procedures for: Shipping Process & IT Warehouse Survey Process.

**R2:** These procedures are being collected on the "Y" drive and will be posted in our Knowledge Base within UniCenter. \*\*\*\*\*

**CLOSED**

**6 Month Response:**

**R1:** The IT Warehouse is working on their final procedures that need to be written. (Survey and Shipping Procedures)

NOTE: ((\*\*)) Indicates confidential and/or proprietary information redacted (Government Code section 6254.9).



### 1 Year Update

**R1:** The IT Warehouse has completed all procedures as requested. The procedures have been posted to our knowledge base and are stored on our "Y" drive folder. **CLOSED**

**SD Owner:** Larry Walker

**SD Status:** **CLOSED**

**SD Resolution:**

### 60 Day Response:

**R1:** Procedures for requesting loaner laptops are completed and available for staff. **CLOSED**

**R2:** Procedures for requesting loaner laptops are completed and available for staff. **CLOSED**

**F8** – Some IT equipment are not locked in secure areas when not in use.

**R1:** Once equipment is identified as needing to be returned to the IT Warehouse and is picked up by an IT Service Desk technician, UniCenter should be updated and the equipment taken directly to the IT Warehouse for storage.

**R2:** All IT equipment transactions should be updated in UniCenter by the IT Service Desk technician immediately after equipment is picked-up from/delivered to the IT Warehouse, training rooms, individual workstations, storage areas, etc.

**R3:** The location code should be updated immediately after being moved/transferred.

**R4:** Any lost or stolen equipment should be reported to Worksite Security immediately once it is identified as missing

**SD Owner:** Lori Sanfilippo

**SD Status:** **CLOSED**

**SD Resolution:**

### 60 Day Response:

**R1:** This is being done and documented by a process flowchart. This flowchart is completed and will be published in the Knowledgebase. **CLOSED**

**R2:** This is currently not being done by deployment staff as current staffing levels do not allow for this additional step to be performed. As asset management tools are improved and processes refined, efficiencies realized can be used in this effort. Additionally, "right in time" deployment greatly reduces the gap in time between the assets leaving the warehouse to the deployment to the end user. A crystal report may be created to identify assets in transit to help reconcile inventory.

**R3:** This is being done by the OAR Deployment staff upon delivery of the asset to the customer. **CLOSED**

**R4:** This is currently being done by all staff and documented in Knowledgebase article 40280. **CLOSED**

### 6 Month Response:

**R2:** This report has been requested but not completed as of yet.

### 1 Year Update

**R2:** The monthly report was created and has been in production since 6/1/2009. **CLOSED**

**F9** – Separation of duties does not exist in regards to the IT warehouse performing their own physical inventory on IT Warehouse equipment

**R1:** An individual who does not work in the IT Warehouse should be performing the physical inventory.

**ITAM Owner:** Bill O'Brien

**ITAM Status:** **CLOSED**

**ITAM Resolution**

### 60 Day Response:

**R1:** This practice has been changed and the physical inventory of the IT Warehouse equipment will now be conducted by the HW Management and Compliance staff. (See F2-R3 above) **CLOSED**